Appendix A: Detail of Architecture Principle

General Architecture Principles

These principles cover generalized, enterprise wide concepts, which in most instances are common sense, or at least common knowledge, but should be iterated none the less for clarity and completeness.

The general principles should apply universally, to any part of the Department of Commerce. They are guidelines and mandates that encompass basic concepts of the use, design, and management of automated information systems. Most are from lessons learned over many years, from the accumulated wisdom or trial and error. Some are based on specific statutory requirements handed down either from Congress or the White House. In either case, the level of compliance with these principles should approach 100 percent.

Principle GP1

All systems and applications should adhere to Department and Federal privacy standards and these standards should be available for users to read.

Rational

Privacy is essential to the conduct of business. Standards have been mandated at the Department level, and government wide, to safeguard the privacy of the system users. It is imperative to the integrity of the system that it implements all privacy requirements. Further, the standards must be readily available to the user for study. Many systems require users to enter sensitive information about themselves or families, and the confidentiality of the data directly relates to how people will use the system. If they do not trust the confidentiality of the system, they will not use it as intended or required. If they have a strong level of confidence in the integrity of the system, they are far more likely to put personal information into it.

Implications

This principle will require work on the technical infrastructure as well as in the business process. It mandates that digital encryption be employed to render the data difficult or impossible to intercept and translate. It also requires the use of digital certificates to authenticate user transactions, and digital signatures to verify the transactions. Further, it will necessitate the creation of user classes to control access to data, granting access to data on a need to know basis. Additionally, databases and other types of data stores will need to be included in this access control. Any form of storage that cannot provide the required level of security must not be used for any sensitive data.

The business process must also be examined and safeguards incorporated to require that any paper documents containing sensitive information be kept in a secure fashion, and the final disposition of these documents provide for maintaining the proper level of security.

Principle GP2

Data and systems should be protected from malicious attack or other unlawful incursions commensurate with the potential harm and potential risks that would result from loss or misuse of the systems or data.

Rational

Security is the key to privacy and to data integrity. As more systems and applications are deployed via Internet/Intranet, the risks increase. Additionally, as systems become more integrated, the potential for cascading effects from attack increase. Systems and data must be protected from malicious attack, accidental or purposeful misuse, and other forms of danger. The degree to which these measures are implemented depends on how important and critical the systems and data are. Security measures must protect the systems and data, but not impede the users from accomplishing their tasks. This is a common sense application of Department policy to protect all systems and data, without compromising its use or accessibility by authorized users.

Implications

A clear, concise hierarchy of security levels should be developed by the Office of the Secretary, explaining in detail the precautions and restrictions pertinent to each level, and how they should be applied. Additionally, performance measures should be developed to determine how effective these measures are over time, as risks change. Security audits should be conducted at regular intervals to ensure that all proper precautions and safeguards are being applied.

An additional point is that all Web sites should be registered with the Office of the CIO, and a security audit conducted prior to deployment of the site. Many Web sites are built by staff with no particular knowledge of the risks and countermeasures available, and thus greatly compromise the entire enterprise.

Principle GP3

Common business processes will be implemented in a consistent fashion to maximize interoperability and reuse, and minimize user-training requirements.

Rational

There are many tasks that are common throughout the Department. Most of these are administrative tasks, and can be standardized. This does not require centralization of tasks, but implies these tasks can be done using the same tools and processes.

Standardization of these tasks provides several benefits. First, it allows the Department to leverage procurement and development by applying it across the entire organization. This results in volume discounts on hardware and software licensing. Additionally, it simplifies maintenance and reduces the overall cost by minimizing the number of contracts required.

A second point is that by performing common tasks in a consistent fashion, the systems become more reliable, because they are using software components that have been proven in production over time. Data exchanges between systems become simpler as definitions of meta-data are standardized.

Lastly, consistent approaches to user interface functionality will reduce user-training requirements, as they become familiar with a common look and feel over time. This allows training to concentrate on new functionality, and not basic computer skills.

Implications

Applications can be divided into two layers. The first layer is the functionality specific to the task. The second layer consists of operations that are common to all tasks, such as workflow, digital security, directory services, electronic messaging, and data dictionaries. These common functions will be deployed once and all applications will make use of them as needed. This will require specific standards for interfaces between component parts, but the overall benefit will be greater flexibility, more consistency in approach, and software that is more reliable.

Principle GP4

All information system activities shall be conducted in accordance with all applicable laws, orders and regulations.

Rational

The credibility of the Office of the Secretary depends on its adherence to all applicable laws, Presidential orders, and OMB and other regulations in the conduct of its business. The mission of the Office of the Secretary cannot be accomplished if there is mistrust based on abusive behavior or disregard of established operating requirements.

The Department has an established code of conduct, as well as guidelines for acceptable use of information systems. These should be reviewed periodically for relevancy, and communicated to all employees.

Implications

Much of the work of the Office of the Secretary is carried out under various mandated, from Congress, the President, or from OMB. All systems should adhere to the strict letter of the law in the manner that tasks are performed, and they should adhere strictly to the charter under which they operate.

Most administrative systems come under periodic review, and sufficient documentation to demonstrate the adherence to the goals and regulations of the system should be included in the system documentation.

Principle GP5

All applications deployed to the Office of the Secretary or to the public should be accessible by persons with disabilities to the extent possible.

Rational

The broad interpretation of the Americans with Disabilities Act must be accounted for in all system development performed by the Office of the Secretary. In short, any system that provides products and/or services to the end user should also provide the capability for persons with disabilities to use those systems.

Implications

The Office of the Secretary should develop a working group to define guidelines to assist developers in this effort. There are vast numbers of resources available, and these should be used to aid in this effort.

Additionally, systems that are covered under this law should be identified, and a timetable should be established for bringing each one into conformance.

Principle GP6

System development and procurement should conform to a coherent set of Open System standards adopted by the Office of the Secretary.

Rational

True interoperability is one of the prime motivations in developing an architecture plan. To accomplish this, system components must be controlled based on established Government and Industry standards that define the interactions and interrelations of the components. This applies to hardware, software and telecommunications.

Implications

The Office of the Secretary should define or adopt such standards as required to assure that all systems can interact with minimal transformation, interpretation, or reliance on intermediate processing steps. Many of the required standards already exist as de facto standards. Most of the other standards required have been developed by various recognized organizations (ANSI, ISO, IEEE etc…) and should be evaluated for applicability. The use of standards should not restrict choices or inhibit development, but rather direct it towards a common goal.

Business Architecture Principles

Business principles cover the use of IT systems as they relate to the business processes. They are concerned with how IT is used, and how the business processes is impacted by IT systems.

These principles are also common sense guidelines that put the enterprise into perspective by placing the business process as the driving force and not the technology used to perform the tasks. They are an affirmation that technology should be used to improve business processes. This replaces the idea that business should change to make use of new technology, even if no business case can be made to support the change.

Principal BP-1

Data should be captured electronically at the earliest possible point in a process, and never be transcribed to move between applications or systems.

Rational

Data transcription errors are one of the most common sources of problems in any automated system. Each time a person has to read data from paper and key it into a system, there is a chance that errors will occur. The more often data is transcribed the more likely an error will occur. Many errors can be checked for by validation of allowable ranges of values, however many types of data do not lend themselves to this form of verification.

To minimize the possibility of errors, data should be captured electronically as close to the source as possible. Any individual transaction should be accomplished by means of electronic forms, capturing data as it is entered. For data sent from outside sources, it should be verified and stored without transcription.

A second major cause of error is multiple sources of the same data. Only one database should maintain the integrity of any piece of data. In other words, any use of the data by other systems should always go to the originating system for the data, and should return any changes of that data back to the origin. In this way, multiple updates to the original data are applied to the source, and do not propagate different changes in different locations and thus destroy the integrity of the source data.

Implications

The OSEC should work to eliminate the use of paper forms to the maximum extent possible, and instead provide users access to Web based systems which perform the tasks needed. Where specific forms are required, they should be implemented electronically, and all data entered should be validated to the extent possible for allowable range of values, validity of information, and completeness of the information. Once entered, it should be routed to required parties, and all processing should be performed electronically.

Principal BP-2

Applications should be integrated only to the extent required by the business functions they perform.

Rational

There are several levels of system integration possible in today's environment. The tighter systems are integrated, the faster and more seamless they work. However, there are also drawbacks to tight integration, which include rapid propagation of errors, difficulty in problem resolution, and near impossibility of performing upgrades in any reasonable time frame.

The determining factor in level of integration must be business need. There are many instances where very tight integration is required, such as running a nuclear reactor. There are also many instances where it is not required. A common sense approach should be adopted, which provides the best service to the user community, with the least amount of risk and cost.

Implications

A careful and detailed study of the interactions between all systems should be performed, and after analysis of the information, a plan for developing the integration links between systems should be initiated. As part of this plan, detailed interfaces should be defined for each system, and standardized throughout the enterprise.

Principal BP-3

System development should be driven by business case analysis.

Rational

All new system development or upgrades to existing systems should be driven by business case need, and not just because the technology exists. In many instances, new systems are purchased and implemented because end of year money had to be spent. For most of these systems, no true business need existed to justify the expenditure. Each system inaugurates recurring annual expenses, which eat into the ability to acquire systems that are needed to perform required tasks.

Implications

The organizations strategic plan should be used to guide which proposed systems are implemented based on the goals of the organization. The development of linkage between the IT Plans and the Architecture plans are important to the success of the organization. Prior to any expenditure for hardware, software or other components, a full business case analysis should be performed, and the results of the analysis should determine the expenditure.

Principal BP-4

Operational units should be fully engaged with IT staff in specification and selection of applications.

Rational

The development of any system should be done with the full participation of the operational unit(s) that will use the system. They should work with IT planners to make sure that business rules for the system are defined, system requirements are developed and realistic, and user interfaces are developed which support the work to be done in the most efficient manner for the users.

Imperative to the success of any system is how well the end users accept it. If it does not meet their needs, or is difficult to use, or is unreliable, the users will find other ways to perform their tasks, bypassing the system and dooming it to failure. By including them in every step of the process, many common problems can be avoided, the system will live up to user expectation, and have a much higher probability of success.

Implications

Cross-functional teams should be established for the duration of the development process. The teams should consist of operational managers, IT staff, and end users of the system. A requirements document should be developed, in full coordination with the line managers and end users, and this should be used as the verification of functionality once the system is delivered.

Principal BP-5

Applications and Data should be available to users regardless of physical location.

Rational

Technology has removed location dependence as a restriction on use of system resources and manipulation of data. This advance should be utilized to the maximum extent practical to facilitate user access regardless of location. All proper and mandated security and authentication guidelines must be upheld, but within this context, access should be allowed regardless of physical location. Users should be able to access any system that they are authorized to use, and perform their tasks as if they were sitting at their own workstation.

Implications

Secure means of accessing OSEC data and systems should be developed, and system design should take into consideration the use of such devices as palm tops and cellular telephones as alternative means of accessing the Department Intranet.

Data Architecture Principles

Data architecture concerns the data resources required to perform business functions. This architecture is tied closely with the business architecture in that it is the currency used to run the organization and perform all required tasks. The basic components addressed here are collection, maintenance, security, and data integrity. Also addressed is how data is transformed into information.

Principle DP-1

Data exchanges should either be direct, or use tagged file formats.

Rational

When data is exchanged between systems, it should be read from one and written directly into the data storage (database) of the other. Alternately, it should use a tagged format file (such as SGML or XML) so that not only the data, but also its definition is available and documented. A second reason to stipulate this is in conjunction with BP-1, eliminating data transcription as a means of movement between systems.

When direct exchanges between existing SQL compliant databases are possible, it eliminates time delays, and guarantees that the transaction has been successfully completed, or that it did not occur at all (known as two-phase commit). This means data integrity is maintained at all times, and there are no ambiguous states in case of system failures during the transactions.

The alternate of using XML or SGML does not provide this level of integrity, but does assure the user that data definitions are consistent across applications. It allows for direct comparisons, as well as eliminating side effects from format conversions.

Implications

Direct data exchanges using database links should be developed where possible and appropriate. In all other cases, standardized formats for each data file should be developed and documented, and be used universally to minimize errors and development time.

Principle DP-2

Data archive and disaster plans should be developed and implemented to cover all significant data stores, from the desktop to the datacenter.

Rational

All information and data used in, or vital to business tasks performed by the organization should be backed up as often as it changes, and periodic backups should be taken to designated offsite storage locations for disaster recovery purposes. Data is the most critical component of any IT system in that it cannot be replaced like hardware or

software. It is what drives business, and is essential to the operations of the business. For these reasons, it must be managed carefully.

Data falls into three primary groups, static, infrequently changed, and frequently changed. Each type has its own requirements as far as backup frequency and archiving. Static data does not change, so once backed up, it is secure. Infrequent change is on the order of weekly or longer between updates. A backup strategy must be devised to capture changes as close to the occurrence as possible.

Frequently changed data is daily or more often. This data is usually found in transactional systems, such as accounting general ledger or others. Since changes occur more frequently than is reasonable to perform a backup, other options should be employed. The most common is a journaling mechanism, either in an RDBMS, or on the file system itself. Using this technique, all changes are recorded in a journal file, as well as the data source itself, and the journal file can be applied to the last full backup to bring the data source forward in time to the last completed transaction. This along with daily backups, provides a means of restoring all completed work in a predictable fashion, which is vital to maintaining the integrity of the data.

Implications

A comprehensive strategy should be developed for each system to guarantee that data is not lost due to system failure or operator error. The method devised should be the most reliable for the level of risk associated with catastrophic loss. Once developed, the plan should be implemented and all operational personal, both system and operations, should be fully aware of the use of the plan.

Principle DP-3

Data updates must maintain the integrity of the data.

Rational

Data integrity is critical to the function of any system. Without it, the information derived is meaningless. In batch update systems, generally a single process will act on the data, and integrity is not compromised. In interactive systems however, many users can be modifying data simultaneously. The problem this poses is that one user could read a data item, and before making a change to it, another user could change the value. When the first user makes a change, they may not be aware of the other changes, and the second user's changes are eradicated without any consideration. A good example would be a conference room reservation application:

> *Person A brings up the schedule for room 102 and notes that it is not busy. While this is going on, Person B books the room for the entire day. Person A, unaware of the changes, reserves the room for two hours, and in the process, cancels Person B's reservation, without even knowing it.*

This is obviously a non-acceptable situation. To avoid this, the underlying data store must be able to force the users to re-read data that has changed since it was last retrieved. This forces the user to examine the new values and base decisions on that data, instead of the original values they saw.

Implications

For data used in any decision-making or transactional type system, consistency must be maintained. This can be done using any fully SQL compliant database, which has as a core function the maintenance of consistency. It can also be implemented programmatically, however this is much more difficult and costly to do. In short, if the data is important, it is necessary to manage it properly.

Principle DP-4

A data dictionary should be developed and its use enforced for all common data elements.

Rational

A data dictionary is a tool that is used to define and describe data elements. It provides information to programmers in particular, as to what type of data it is (ie: date, character, numeric etc…), which is critical in developing applications that use the data. It also provides information as to what the data element is or what it contains, and how it relates to other data elements. This information is called Meta data, or data about data (a term that confuses most people). As data sharing between systems increases, it becomes more important to standardize the definitions of common data elements to facilitate this sharing. The mechanism to do this is the data dictionary.

Implications

The Office of the Secretary should develop a data dictionary for all data elements that are used in multiple systems, and enforce the use of these definitions when systems are upgraded or replaced.

Additionally, for legacy systems, interfaces should be developed to access the data dictionary and output data items according to the standard format for exchange with other systems.

Principle DP-5

All data should be captured explicitly, there should be no implied information based on context.

Rational

In many instances, data elements that have a finite range of values are used as logical tests in programs. If the value is *x* then execute the following, otherwise execute another section of code. Frequently, when these data elements are defined, there are no constraints placed on the allowable values. This leads to situations where the most common response is entered explicitly, and if there is no response, or any other value, it is treated as the opposite case. When new applications are built using this data, the lack of explicit values can cause unwanted side effects, or program failure. Additionally, a non-response does not convey any information and creates ambiguous situations. The worst case is when a value for one element is inferred by another. This can lead to many ambiguous situations, and significantly degrade the accuracy and validity of the information generated from the data.

Another common problem is a data element that is actually several values in one field. Depending upon the position in the field, the value has a certain meaning. The real peril here is that if the key is lost or forgotten over time, the data becomes totally meaningless.

Implications

As a rule, any data elements that have a known range of values should check for allowable entries. Further, if a response is required for a data element, it is important that an explicit value be entered. One of the most common causes of programs aborting is data containing null values or blanks where numeric information should be. A simple integrity constraint, either at the database or application level, can eliminate these problems and greatly enhance the accuracy and validity of the data.

Additionally, data elements should contain one and ONLY one piece of information about the item to which it refers. The practice of encoding location information in a large field, containing up to 30+ characters is a good example. Not only is it problematic for maintenance, but it also dramatically diminishes the ability to search the data. Each item should have its own definition, and be stored independently of all other items. Modern database designs can maximize storage and retrieval, and the data can still be output in any fashion desired.

System Architecture Principles

Principle SP-1
Each application should clearly specify input data formats

Rational

A very time consuming and error prone task in developing system interfaces is determining what data the receiving system is expecting, in what format, and in what order. If the data feed is by file, I/O errors often occur that crash the program and disrupt timely processing. If the data feed is direct, both systems could crash, and in rare cases, cause corruption of the data source.

In many cases, the output of one process is the input to another, so in most cases, only the input needs to be formally documented and controlled. If the output is not going to another system, the only other destination is reports, and the format for those vary with the user requirements.

Implications

To eliminate this problem area, each system should clearly document the format for all input data. This includes the data type, length, order of data elements, plus any parameters the system requires to perform the tasks it is designed to do. For interactive applications, this information should be available in the help file, which should be included as part of a complete application. Additionally, all programs should scan the input prior to actually processing it, in order to eliminate bad records. Bogus parameters to programs are one of the more common forms of security breaches. By analyzing the content first, the security holes can be filled, and attacks on data and systems thwarted.

Principle SP-2
Applications and software tools should be Web enabled and platform independent.

Rational

One of the major initiatives of the Office of the Secretary is to provide all users with access to systems through the Internet and the World Wide Web (WWW). To this end, all applications should have Web enabled user interfaces. Additionally, to minimize maintenance issues and maximize availability to all users, the user interfaces should be platform independent, that is, they should operate *as is* on any compliant browser, regardless of the underlying operating system or hardware platform.

To further enhance the availability of these systems, the applications should, to the extent possible, be platform independent as well. This would enable the application to be hosted on the most cost-effective platform when it is deployed, and moved at a latter time to a different platform with out the need for significant reengineering. There are many such

products and tools available in the market place today and the number will continue to grow over time. Selection of these tools positions the Office of the Secretary to maintain its investment in applications and tools, regardless of the trends in the hardware segment of the market.

Implications

All applications deployed henceforth should be required to be Web accessible. This means that the end user can access the application using any browser that complies with the current standards (as defined in the OSEC Standards Profile). Any compliant browser will be able to access the application, therefore the client side will be platform independent by definition.

The application itself should be constructed with modular components, and using tools that comply with standards as defined for portability. This should allow the application to be moved between platforms with a minimum of trouble and downtime. The tools selected should be state of the art such as, but not limited to, Java, XML, or other such platform independent tools.

Principle SP-3

The incorporation of COTS software MUST NOT inhibit integration, scalability, or portability.

Rational

Computer of the Shelf (COTS) software has become the most cost-effective means of deploying many applications. The are no development costs, integration costs are moderate, and maintenance costs are much cheaper than performing the same tasks with in-house technical staff.

The other side of using COTS packages is the degree to which they inhibit integration, scalability and portability. Many COTS applications keep initial costs down by employing database packages that do not have all the features of the more robust packages such as Oracle or Ingress. Many of these databases are not fully SQL compliant and some are completely non-compliant. Additionally, many of the applications based on these databases do no have an Application Program Interface (API). An API allows programmers to access the application and data store from programs they write, to provide functions the COTS package does not include, and to integrate the package with other components or systems. Without an API, the package is essentially useless in that integration with other packages and applications is complicated at best, impossible at the worst.

Many COTS packages are built to run exclusively on Intel based platforms, and are designed for the low end of the market. They may work well for a small office or business, but when applied to a large number of users, they simply fall apart. This is scalability. A COTS package must work just as well for 5000 users as it does for 50. If not, it simply causes more problems and downtime than it is worth. There are no real

saving realized when productivity is negatively impacted by poor performance and down time of the systems. A major goal of the OSEC is to leverage cost of systems by standardizing on one per application area, and saving on license fees and maintenance costs. If the package does not scale to the user community it is deployed to, it is not acceptable.

Portability is the ability to move an application from one platform to another without major reengineering of the software. This allows the OSEC to get the most value for the dollar on hardware purchases without being constrained to a particular platform or vendor. COTS applications should either be platform independent, or be available on a number of platforms, so that hardware procurement is not directly coupled to what software is to be employed. There are many instances where this may not be possible, but it is a criterion that should be evaluated for all COTS purchases.

Implications

A technical reference model that clearly delineates the role of the system wide services (messaging, workflow, data dictionary, PKI, and directory services) vs the applications should be developed. It should contain clear, concise interface requirements for each standard package. All applications must be able to communicate with these packages as need, to fulfill their function.

Secondly, scalability tests must be defined for each application, and must be incorporated into acceptance testing. Along with tests for ease of integration and portability, these tests should be performed before even measuring adherence to application specific requirements. If they do not pass these tests, it does not matter if performs the work or not, it will fail when deployed to the whole Department, or any sizable subset of it.

Lastly, a document should be prepared detailing the general mandatory requirements for all enterprise wide COTS applications. These should be included in any procurement package and should be strictly adhered to.

Principle SP-4

All applications must be capable of interacting with all security applications, such as digital certificate, public key encryption, and digital signature where applicable.

Rational

To construct a true Digital Department, a means of authorizing transactions electronically is critical. It is also vital that the information is secure and privacy maintained. Digital certificates and digital signatures are a means of performing authorization and verification electronically, and public key encryption is a means of encoding data such that it is not readable by persons surreptitiously intercepting data transmissions.

Implications

All applications deployed for administrative functions in the OSEC must have the ability to interact with digital certificates, public key encryption, and digital signatures where applicable. This will allow the automation of the workflow, maintain the authenticity of the information and preserve the privacy of the users as the Digital Department is deployed.

Principle SP-5

All system must be maintainable and reliable (some components must be 24x7)

Rational

Electronic Commerce by its nature is a 24 hour a day, 7 days a week operation. Many of the functions to be provided will be available 24x7. The applications must be robust, and provide means for maintenance with minimal impact on availability. The must also make use of existing hardware to perform backup and recovery operations.

Implications

The applications and systems that are most critical, as defined by operational managers, must provide the ability to operate around the clock, and still provide a means for performing backups and other routine maintenance procedures. Additionally, vendors must be able to respond in a timely manner with software patches for bugs in the application. Failure to correct a problem on a critical system will cause serious downtime, as the system will must likely be unstable and incapable of performing reliably enough to allow work to progress.

Principle SP-6

All systems should include full documentation, disaster plans, and provide a means to backup all critical data.

Rational

No application system is complete without full documentation, including a disaster and recovery plan and routine maintenance plans. Requirements differ from system to system, but each should have a fully documented plan, and procedures to implement the plan.

Documentation is critical in that it provides maintenance staff the means of finding the causes of problems, as well as a blueprint of the system to enable them to make minor enhancements over time.

Implications

The OSEC should establish a review procedure for all new application systems, and as part of that process, should evaluate the documentation and backup/recovery plans. Additionally, it should review the ability to perform the backup or recovery in a timely manner. Sufficient capacity must exist to perform these functions, as they are as critical to the long-term success of the system as any other factor.

Infrastructure Architecture Principles

The IT infrastructure consists of the hardware, operating systems, communications services, user workstations, and application services. These components provide not only the basic requirements for hosting an application, but also the means of integrating the application into the enterprise as an integral component. The software tools used to build the applications, such as compilers and code development tools are essential parts of the infrastructure, and the level of standardization these tools adhere to will impact on hardware procurement flexibility.

Principle IP-1

Primary servers should provide sufficient redundancy to ensure that work is not lost or delayed due to equipment failures.

Rational

The primary servers employed for application hosting, directory services, security services, and electronic mail are critical to the normal functioning of the organization. With one or more of these servers unavailable, work becomes difficult or impossible to perform. As tasks and application become more integrated over time, failure of a single component could jeopardize all systems.

Implications

The OSEC should evaluate the critical nature of each server, and design sufficient redundancy into the infrastructure such that work can be performed even if there are outages or downtime on specific servers. Additionally, it should assure that staff can be notified immediately when problems arise, so that they can begin corrective action quickly. Lastly, service contracts with vendors for critical systems or system components should be on a 24-hour per day basis, to minimize downtown waiting for repairs.

Principle IP-2

Network hardware should provide sufficient bandwidth to minimize data transfer delays and user timeouts.

Rational

As more applications are hosted on the Intranet, and more business is conducted through the Internet, the network becomes the system. Large quantities of data and information will be flowing through the telecommunications equipment, and it must provide sufficient bandwidth to accommodate the load. It must not only be able to carry the normal workload, but have reserve capacity sufficient to cover periodic peaks well above the average. As is true in all other facets of automation, if the process slows the work, users

will find alternate ways to perform their tasks, often to the long-term detriment of the enterprise as a whole.

Implications

An extensive analysis of the demands on the network should be performed, and this information should be used in gauging the equipment requirements for the Intranet.

Principle IP-3

All system and network hardware should conform to industry wide standards, and use of-the-shelf components.

Rational

Industry standards for hardware and networks have enabled the integration of systems to form an enterprise wide system. They have also catalyzed much of the growth of the Internet as well as the end user desktop environment. Most hardware currently available conforms to some level of interoperability standards, as do most modern networks. It is critical to maintain and even expand this within the enterprise, to promote further growth and capabilities.

Implications

The OSEC Standards profile should contain standards for hardware, networks, and associated software. It should require all procurements to conform to these standards unless sufficient justification can be made, including certification that security and interoperability will not be compromised by using non-compliant products.

Principle IP-4

Navigation of the Intranet should be transparent to the end user, all applications and services should be available without requiring the user to know their location.

Rational

One of the primary weaknesses of most corporate or government web sites is that they are segmented along organizational lines. This requires the potential user to have prior knowledge of the organization to find the information or application they are looking for. This can be a very tedious and time-consuming task, and discourage users from accessing the system at all. It also requires additional expenditures since each organization maintains its on Web presence.

Implications

Web sites should be characterized and organized by function rather than organizational division, and navigation should require as few levels as possible to find the desired page. Additionally, care should be taken in designing pages to allow frequently accessed pages to be bookmarked, as well as stored in cache on the Web server for faster retrieval.

Principle IP-5

Firewalls and other security features should be employed to the extent required to meet Federal and Department requirements.

Rational

Network and information security is vital to the smooth operation of the OSEC. As more tasks are propagated to the Intranet/Internet, vulnerabilities will increase and be tested by hackers. Use of software tools that provide remote access, but violate security regulations and procedures should be discontinued.

Implications

The Federal government has defined requirements for security, as well as the Department of Commerce. ALL systems must comply with these security requirements and should be evaluated for compliance prior to deployment. Additionally, an IT security plan should be developed for each system, documenting measures taken and responsible parties to notify when problems occur.